



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,665	10/10/2003	James Edward Aston	RSW920030166US1	1807

7590 12/28/2007  
David R. Irvin  
IBM Corporation T81/503  
PO Box 12195  
Research Triangle Park, NC 27709

EXAMINER
----------

TRAN, TONGOC

ART UNIT	PAPER NUMBER
----------	--------------

2134

MAIL DATE	DELIVERY MODE
-----------	---------------

12/28/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/683,665

Applicant(s)

ASTON ET AL.

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 28 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-10 and 30-39 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10 and 30-39 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. This Office Action is in response to Applicant's Amendment filed on 9/28/2007. Claims 1-12 have been amended. Claims 11-29 have been canceled. Claims 30-39 have been added. Claims 1-12 and 30-39 are pending.

### ***Response to Arguments***

2. Applicant's arguments with respect to amended claims have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 2, 5-7, 9, 10, 30, 31, 34-36, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yaidya (U.S. Patent No. 6,279,113) In view of Hypponen (U.S. Patent No. 6,577,920).

With respect to claims 1 and 30, Yaidya discloses a method and a computer-readable medium having a computer program product for performing virus detection on a file within a computer system, said computer-readable medium comprising:

Computer program code for categorizing a plurality of virus signatures into a respective one of a plurality of anti-virus sets according to their characteristic, wherein each of said anti-virus sets contains virus signatures sharing at least one common characteristic (Yaidya, e.g. Abstract, col. 3, lines 12-16, network object corresponds to executing agent);

Associating an executing agent with a subset of said plurality of anti-virus-sets, wherein said executing agent is associated with a target file (Yaidya, e.g. col. 1, lines 34-44 and col. 3, lines 34-39); and

Yaidya discloses in response to said target file being opened by said associated executing agent, processes the content of said target file for viruses by applying virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent (e.g. Yaidya, col. 1, lines 34-44 and col. 3, lines 40-48) .

Hypponen discloses scanning software file for viral infection against different signature databases (Hypponen, e.g. col. 3, lines 14-16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the categorizing of plurality of virus signatures and subset of virus signatures taught by Yaidya with scanning of files from different signature database to detect and identify viral infection to alert and protect user's from virus attack (e.g. Hypponen, col. 3, lines 14-20).

With respect to claims 2 and 31, Yaidya and Hypponen further include wherein said target file being opened by said associated executing agent is performed by an operating system (Yaidya, e.g. col. 1, lines 34-44).

With respect to claims 5 and 34, Yaidya and Hypponen further includes marking said target file has been scanned and allowing said target file to execute in response to a determination that contents of said target file do not match any virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent (Yaidya, e.g. col. 3, lines 12-48).

With respect to claims 6, 7, 35 and 36, Yaidya and Hypponen do not specify taking the action of quarantining or deleting said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent. However, Official Notice is taken quarantining or removing infected file is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to delete the file after the system determine that it has been attack to protect resource from further damaged.

With respect to claims 9, 10, 38 and 39, Hypponen discloses wherein the plurality of anti-virus sets have a first anti-virus set and a second anti-virus set, Hypponen further discloses the organizing step further comprises:

arranging the plurality of anti-virus sets into a hierarchical structure having first and second levels, the first level having the first anti-virus set containing virus signatures which are mutually applicable to a plurality of executing agents (e.g. col. 3,

lines 17-20), Hypponen does not explicitly describe the second level having the second anti-virus set containing virus signatures which are exclusively applicable to the first portion of the plurality of executing agents or a third level having the third anti-virus set containing virus signatures which are exclusively applicable to one of the first portion of the plurality of executing agents.

However, Hypponen describe a type of virus consisted of a piece of executable code which attached itself to a bona fide computer program that typically inserted a JUMP instruction into the start of the program which when the program was executed, caused a jump to occur to the “active” part of the virus (Hypponen, col. 1, lines 15-19).

Vaidya discloses a dynamic signature-based network intrusion detection system includes multiple attack signature profiles which are each descriptive of identifiable characteristic associated with particular network intrusion attempts associated with network objects located on the network, the attack signature profiles can include *generic attack and/or customized attack signature profile* (e.g. Vaidya, col. 3, lines 12-38). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Hypponen’s describing a certain virus that attach *in the start of a program* to trigger the virus code to activate in a software program with Vaidya’s teaching of generic and/or customizing attack signature into different signature profiles to improve the virus detection system in way that efficiently associating identifiable characteristic with particular network intrusion attempts and network objects (Vaidya, col. 3, lines 34-38).

4. Claims 8 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (U.S. Patent No. 6,279,113) in view of Hypponen (U.S. Patent No. 6,577,920) and further in view of Sarkar (U.S. Patent Application Publication No. 2004/0158730).

With respect to claims 8 and 37, Vaidya and Hypponen do not disclose a periodic scanning said target file associated with said executing agent. However, Sarkar discloses a set of program instruction in a program module invoking file scanning for anti-virus protection according to periodic job schedule (Sarkar, [0064]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement file screening protection by grouping macro virus signatures into different databases taught by Hypponen with a program module to invoke periodic scanning according to job schedule taught by Sarkar as part of file protection maintenance.

5. Claims 3, 4, 32 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yaidya (U.S. Patent No. 6,279,113) In view of Hypponen (U.S. Patent No. 6,577,920) and further in view of Mclchionc (U.S. Patent No. 6,973,578).

With respect to claims 3, 4, 32 and 33, Yaidya and Hypponen do not further include wherein said computer-readable medium further includes computer-program code for defining a rule to preclude scanning of said target file and said rule to preclude scanning of said target file, allowing said target file to execute without scanning said target file for viruses. However, Mclchionc discloses conditionally scanning files based on a type of file that is being released to a requestor (Mclchionic, e.g. col. 1, line 62-col.

2, line 6). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the technique for conditionally scanning files taught by Iclchionc with categorizing of plurality of virus signatures and subset of virus signatures taught by Yaidya with scanning of files from different signature database to detect and identify viral infection taught by Hypponen to minimizing the amount of system resources used to provide security protection from viral attack (Iclchionc, col. 1, lines 61-66).

### ***Conclusion***

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.



Application/Control Number:  
10/683,665  
Art Unit: 2134

Page 8

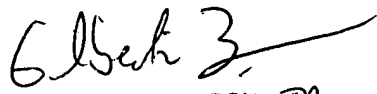
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Examiner: Tongoc Tran  
AU: 2134

December 10, 2007

  
GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100